



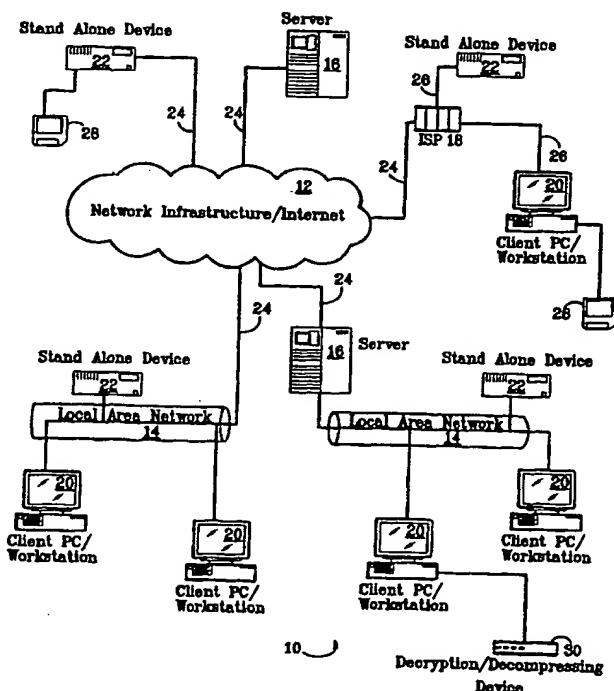
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :  H04L 29/06, G06G 1/00		A1	(11) International Publication Number: WO 99/55055
			(43) International Publication Date: 28 October 1999 (28.10.99)
(21) International Application Number: PCT/US99/08196		(81) Designated States: CA, JP, SG, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 13 April 1999 (13.04.99)			
(30) Priority Data: 09/061,493 17 April 1998 (17.04.98) US		Published <i>With international search report.</i>	
(71) Applicant: IOMEGA CORPORATION [US/US]; 1821 West Iomega Way, Roy, UT 84067 (US).			
(72) Inventors: KUPKA, Michael, S.; 4521 Kenbrook Drive, Nacogdoches, TX 75961 (US). HAWKINS, Michael, L.; 1324 Pruitt Drive #914, Nacogdoches, TX 75961 (US). THOMAS, Trent, M.; 1758 Hillside Circle, Ogden, UT 84403 (US).			
(74) Agents: KURTZ, Richard, E. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP 46th floor, One Liberty Place, Philadelphia, PA 19103 (US).			

(54) Title: SYSTEM FOR KEYING PROTECTED ELECTRONIC DATA TO PARTICULAR MEDIA TO PREVENT UNAUTHORIZED COPYING

(57) Abstract

A system and method for distribution of electronic data over a network infrastructure that includes a client device for operation by a user desiring to receive the electronic data and server that contains the electronic data and offering the electronic data for downloading to the client device via the network infrastructure. The client device communicates a unique identifier associated with a particular piece of media to which the electronic data is to be stored to the server. The server encrypts the electronic data using the unique identifier as a key and downloads the encrypted electronic data to the client computer, where the client computer writes the encrypted electronic data to the particular piece of media such that the encrypted electronic data may only be accessed from the particular piece of the media. An apparatus for reading encrypted electronic data associated to one piece of media by a unique identifier contained on the one piece of media comprises a processor which controls and executes instructions to read the electronic data and the unique identifier from the one piece of media, and a media drive, responsive to the processor, which reads the unique identifier and the electronic data from the one piece of media. The electronic data is decrypted for use by the apparatus or another device attached to the apparatus using the unique identifier as a data key, and the data is accessible from only the one piece of media having the unique identifier and is not accessible from any other media having a different or no identifier. In an alternate embodiment, the apparatus for reading the encrypted electronic data is connected to a general purpose computer having a media drive which reads the unique identifier and the electronic data from the one piece of media. The apparatus comprises an application specific integrated circuit which controls and executes instructions to accept the electronic data and the unique identifier from the general purpose computer.



## **SYSTEM FOR KEYING PROTECTED ELECTRONIC DATA TO PARTICULAR MEDIA TO PREVENT UNAUTHORIZED COPYING**

### **FIELD OF THE INVENTION**

The present invention relates to the prevention of unauthorized copying by associating electronic data to a particular piece of storage media. In particular, the present invention relates to a remote data delivery system wherein electronic data to be protected is delivered in a secure manner to a local machine which stores and permanently associates the protected electronic data to a particular piece of storage media based on a unique key of the media.

### **10 BACKGROUND OF THE INVENTION**

Protection of copyrighted and other protected digitally stored data has always been a primary concern of the owners of such material. In particular, piracy of computer software, music and video has been and continues to be of great concern because it is all but impossible to stop. Although there have been many prior attempts by the software, music, and video industries to curtail piracy, each has been met with limited success.

As part of the effort to combat piracy, software vendors have licensed software rather than transferring ownership when purchased. When software is purchased, the purchaser becomes a licensed user (i.e., licensee) rather than an owner. Copying of software under most license agreements is generally limited to one copy for backup purposes only in

- 3 -

intellectual property, there were few, if any, mass distribution channels. At the same time period, the music and video industries were strictly analog at the consumer level. Thus, piracy was not a major factor as it was limited to small groups of people or organizations. However, with powerful computers on every desktop and the evolution of music and video into a digital 5 format, piracy has become a major factor costing software vendors alone \$4 billion a year worldwide. Clearly, the financial loss to software developers, musicians, actors, and their associated industries is immense.

At the root of the global communications expansion is the rapid growth of the Internet, which has pushed the piracy problem to the forefront. As is well known in the art, 10 the term "Internet" was first used in 1982 to refer to the enormous collection of interconnected networks that use Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. Despite only gaining mass recognition over the past four years, the Internet has existed since the late 1960's and was originally designed as a Wide Area Network (WAN) that would survive a nuclear war. Throughout the 1970's and 1980's a growing number of small 15 networks developed and connected to the Internet via gateways as a means of exchanging electronic mail. In the mid 1980's there was a significant growth in the number of available Internet hosts, and since the late 1980's, the growth of the Internet has been exponential. The growth of the Internet has provided people all over the world with a means to share and distribute information. Thus, the potential now exists for the mass distribution of pirated 20 software, music and video on a global scale. Many Internet Usenet groups and channels on the Internet Relay Chat (IRC) are dedicated to the trading of pirated files, music and videos. Furthering the piracy problem are groups that maintain a high profile and take a great deal of 25 pride in their piracy accomplishments. The piracy problem has grown so large that a new term, "warez," is used to describe the pirates and their activities. The Internet now provides a great potential for legitimate sales and distribution of protected software, music and videos, because of its size, speed and penetration into the homes of consumers. However, these very advantages make it easy for pirates to steal expensive, proprietary software that took years to design and manufacture and within hours make it available to anyone, free for the taking.

In view of the above, there is a need for a secure method and apparatus for 30 electronic distribution of data which will take advantage of the wide distribution of networks such as the Internet, while simultaneously preventing unauthorized and illegal copies of

- 5 -

electronic data and an encryption key to the electronic data. The encrypting of the electronic data is performed using the unique identifier as an encryption key.

According to yet another feature of the present invention, establishing a connection between the client device and the server via the network infrastructure comprises  
5 submitting a form to the server, executing a program to process the form, and sending a metatag and transaction file. The metatag and the transaction file may be used to launch a client program at the client device after being sent to the client device. In addition, the client program may open the transaction file and parse metadata from metatags within the transaction file. The client may connect to a server address identified by a predetermined  
10 metatag in the transaction file to receive the electronic data, and the server address may be dynamically changed as the electronic data is requested from the server.

According to another aspect of the present invention, there is provided a method of accessing electronic data stored on a media by a first device adapted to read the media, where the electronic data has been written to the media in an encrypted format. The  
15 method comprises accessing the electronic data on the media, reading a unique identifier of the media, reading a portion of the electronic data from the media, and decrypting the electronic data using the unique identifier as a decryption key.

According to a feature of the present invention, the reading of the unique identifier comprises reading the unique identifier from a predetermined track of the media.  
20 The reading the unique identifier of the media may further comprise communicating the unique identifier to a second device, and the reading at least a portion of the electronic data further comprises communicating the portion of the electronic data to the second device, wherein the second device performs the decrypting the electronic data using the unique identifier as a decryption key.

25 According to another feature, the method may further comprise communicating an authentication code to the first device, reading the unique identifier from the media, comparing the authentication code to the unique identifier, and if the authentication code equals the unique identifier, generating a verification code which is communicated to the second device.

30 According to yet another feature, the method may further comprise reading a predetermined string from the media, decrypting the predetermined string, comparing the

- 7 -

identifier. The unique identifier may be located on a predetermined track of the one piece of media.

According to another feature of the present invention, the apparatus includes an application specific integrated circuit that performs the decryption. The apparatus may 5 further comprise an analog to digital converter, wherein the application specific integrated circuit decompresses the electronic data and the analog to digital converter converts the decompressed electronic data into audio signals.

According to yet another feature of the present invention, the media drive further comprises an application specific integrated circuit, the application specific integrated 10 circuit of the media drive performs the decryption, and the decrypted electronic data is passed to the apparatus.

According to still another feature of the present invention, the media drive reads a predetermined string from the media, and the processor decrypts the predetermined string and compares the predetermined string with a known string, and the apparatus is halted 15 if the predetermined string does not equal the known string.

According to yet another aspect of the present invention, there is provided an apparatus for reading encrypted electronic data associated to one piece of media by a unique identifier contained on the one piece of media. The apparatus is connected to a general purpose computer having a media drive which reads the unique identifier and the electronic 20 data from the one piece of media. The apparatus comprises an application specific integrated circuit which controls and executes instructions to accept the electronic data and the unique identifier from the general purpose computer. The electronic data is decrypted for use by the apparatus using the unique identifier as a data key, and the data is accessible from only the one piece of media having the unique identifier, and the data is not accessible from any other 25 media having a different or no identifier. The unique identifier may be located on a predetermined track of the one piece of media.

According to a feature of the present invention, the application specific integrated circuit performs the decryption. The apparatus may further comprise an analog to digital converter, wherein the application specific integrated circuit decompresses the 30 electronic data and the analog to digital converter converts the decompressed electronic data into audio signals.

- 9 -

Figure 9 is a flow chart of the processes performed by PC/Workstation or stand-alone machine during the reading/execution/playback of the protected data; and

Figures 10A and 10B are a flow charts of the processes performed by the decryption/decompressing device during the read/playback of data.

## 5 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides for a secure method of transmitting sensitive and protected electronic data (protected content) from a remote server to a client computer or stand-alone device over a network infrastructure and for preventing the unauthorized distribution and copying of the data once it is delivered to the client computer or stand-alone 10 device. As used herein, the term "data" includes all information that may be stored on a storage media, including but not limited to, executable files, linked library files, data files, databases files, audio files, and video files.

Referring to Figures 1-5, there is illustrated an exemplary, non-limiting, environment 10 and devices in which the present invention may be implemented. As shown 15 in Figure 1, the environment 10 includes a Wide Area Network (WAN) infrastructure 12. The WAN infrastructure 12 may comprise a Transmission Control Protocol/Internet Protocol (TCP/IP) network such as the Internet. Attached to the WAN infrastructure 12, via communications lines 24, may be one or more Local Area Networks (LAN) 14, servers 16, Internet Service Providers 18, and stand alone devices 22 that are compatible with the 20 protocols of the WAN infrastructure 12. As illustrated, the LAN 14 and ISP 18 may have attached thereto client PC/workstations 20 and/or stand alone devices 22 that may access the network infrastructure 12 via the LAN 14 or ISP 18, and that are capable of at least accessing and reading data on a removable media 28. Also shown is a data decryption/decompressing device 30, which is attached to a PC/workstation 20.

25 The LAN 14 may comprise an Ethernet or Token Ring network and have a server 16 and gateway (not shown) that provides a connection to the network infrastructure 12 via one or more communications links 24. The communication links 24 to the remote systems may be wireless links, satellite links, or dedicated lines.

The servers 16 may comprise, for example, UNIX-based or Windows NT  
30 Server-based computer platform having one or more processors (e.g., Intel Pentium II

- 11 -

to emphasize that a removable media drive can be implemented in either internal or external form.

The MODEM/Terminal Adaptor/Network Interface Card 82 may comprise individual cards performing communications-related functions, as known in the art. The 5 MODEM/Terminal Adaptor/Network Interface Cards 82 are included within PC/workstation 20 to provide communications to external networks to which the PC/workstation 20 is connected. In particular, the MODEM/Terminal Adaptor/Network Interface Card 82 may be used to access LAN 14, ISP 18 and network infrastructure 12.

Communications between internal and external devices may be accomplished 10 via controllers provided within the PC/workstation 20. A serial/parallel/USB port controller (which may comprise separate controllers) 58, a monitor controller (video card) 60, and a keyboard and mouse controller 62 each provide an interface between the CPU 66 and an external removable media drive 52b (or printer), monitor 54, and keyboard and mouse device 56, respectively. A hard disk and floppy disk controller 72 serves as an interface between the 15 CPU 66 and the hard disk 76 and the CD-ROM drive 80, and the floppy disk 74 and tape drive 78, respectively. It will be appreciated by those skilled in the art that the disk controller 72 may comprise separate floppy and hard disk controllers (e.g., IDE or SCSI controller).

A removable media controller 68 serves as an interface between the removable media drive 52a and the CPU 66. For example, the removable disk controller 68 may 20 comprise a Small Computer System Interface (SCSI) or Integrated Drive Electronics (IDE) interface controller. A hard disk and floppy disk controller 72 serves as an interface between the CPU 66 and the hard disk 76 and the CD-ROM drive 80, and the floppy disk 74 and tape drive 78, respectively. Alternatively, the removable media drive 52a may utilize the disk controller 72 as an interface to the CPU 66.

25 Referring now to Figure 3, there is illustrated a block diagram of an exemplary media drive 52 having a SCSI interface to the PC/workstation 20 (via controller 68). The media drive 52 preferably comprises, a ZIP® drive, manufactured by Iomega Corporation, Roy, Utah; however, other media drives may be used as media drive 52. The media drive 52 includes components that provide for communication between the read/write channel for the 30 media (lower right side of diagram) and the PC/workstation 20 (upper left side of diagram). The media drive 52 includes an AIC chip 101 which performs the SCSI 102, the direct

- 13 -

52) to read the media 28, but rather receives data which is read by, and communicated from, the PC/workstation 20.

Referring now to Figure 5, there is illustrated a block diagram of an exemplary decryption/decompressing device 30. The decryption/decompressing device 30 may be connected to the PC/Workstation 20 via e.g., a universal serial bus (USB) connection, parallel port or serial port to receive the protected electronic data from the PC/Workstation 20 and may output analog audio and video signals via analog communications lines 42 to an external analog input device 44, such as a stereo amplifier, television, video cassette recorder or sound card. The decryption/decompressing device 30 includes a USB/parallel/serial port controller 34, an ASIC/controller 36, a digital to analog converter 38, and RAM 39. The USB/parallel/serial port controller 34 interfaces with the USB/parallel/serial port of the PC/workstation 20 via lines 32 to provide communications between the decryption/decompressing device 30 and PC/workstation 20. The USB/parallel/serial port controller 34 also provides for communication of data between the PC/workstation 20 and the ASIC/controller 36. The ASIC/controller 36 may decrypt the protected data and output digital audio and/or video signals (e.g., Pulse Code Modulation (PCM)) to the digital to analog converter 38 for conversion to analog audio signals.

Alternatively, the decryption/decompressing device 30 may be provided as a card which is installed within the PC/workstation 20. Such a decryption/decompressing device 30 may communicate to the PC/workstation 20 via the internal bus (e.g., ISA, PCI or AGP) of the PC/workstation 20 instead of via the USB/parallel/serial port. Further, the decryption/decompressing device 30 in this alternative configuration would be provided with an interface to enable communications with the internal bus of the PC 20.

It is noted that the exemplary environment and devices shown in Figures 1-5 are not limited to the illustrated environment, as other network infrastructures, communications connectivities, and devices are intended to be within the scope and spirit of the present invention.

Referring now to Figure 6, there is shown an overview of the processes performed in accordance with the electronic distribution model of the present invention. As will become evident to those of skill in the art, the features and aspects of the present invention may be implemented by any suitable combination of hardware, software and/or

- 15 -

the protected electronic data, protecting the intellectual property rights of the seller or owner of such rights.

The overview illustrated in Figure 6 will now be described in greater detail with reference to Figures 7-9. Figure 7 illustrates the download process of electronically distributing data over the network 12 from a server 16 to a client PC/workstation 20 or stand alone device 22. As noted above, the protected electronic data will be downloaded to a particular piece of media having a unique identifier so that the data will be associated with the particular media and accessible from only the particular media.

At step 300 the process begins after a user on the client PC 20 has contacted 10 and connected to a server 16 (Web server) via, e.g., a Web browser, and makes a selection of protected data for downloading. It is preferable, that the Web sever 16 comprises an Iomega store web server 16, which will be described below. It is also preferable that the connection to the Web server is a secure (i.e., encrypted) connection. After the user clicks on the download button of the displayed web page from the Web server, this action causes the 15 PC/workstation to submit an HTML form to the web server 16. The web server 16 then executes the appropriate Common Gateway Interface (CGI) program. The CGI program running on the Iomega store web server 16 sends the metatag "Content-Type: application/x-itf" followed by an appropriate Iomega Transaction File (ITF) to the client PC/workstation 20. The ITF file is unique to the Iomega store web server 16 and is used to provide information 20 to an ITF client program which controls the download process at the client side. The format of the ITF file is shown in Figure 8. As the web browser receives the metatag, it launches the ITF client program and passes the ITF file name as a command line parameter. The ITF client application opens the ITF file and parses the metadata from the metatags. The client PC/workstation 20 connects to the server address provide by the ITFSERVER tag to receive 25 the electronic data (see step 308). The server address may be dynamically changed for each request in order to balance the load on the server. For example, the ITF file may include the following information for a transfer of a single file containing a song:

- 17 -

```
m_DriveNum = 0;  
for(j = 0;j < 26;j++)  
    // scan the drives and find the IOMEGA drives  
{  
5      if(IsIomegaDrive(j) )  
    {  
        k = GetGeneralDevType(j);  
        if( k == DRIVE_IS_ZIP )  
        {  
10       m_DriveNum = j;  
            j = 26;  
        }  
    }  
}  
15  }  
  
void CClientApp::GetSerialNumber()  
{  
    unsigned char szBuffer[1024];  
    memset(szBuffer,0,sizeof(szBuffer));  
20    memset(&m_SerialNumber,0,40);  
    GetInfoNonSense(m_DriveNum,0x02,szBuffer);  
    memcpy(&m_SerialNumber,&szBuffer[22],39);  
}
```

It can be appreciated that the unique identifier is not limited to information  
25 stored on the media 28 such as the serial number, and that other types of information could  
be used as the unique identifier. In addition, the unique identifier should contain a sufficient  
number of bits (length) to ensure that no two pieces of media have the same identifier. For  
example, each Iomega ZIP® disk contains a unique 39 byte (312 bits) serial number, and other  
bit lengths may be utilized.

- 19 -

At steps 306-310 the client sends a command packet with an action code of two (step 306), which informs the server to send the next 4000 bytes of data encrypted the unique identifier. This action code is repeated until the entire file has been transferred from the server 16 to the client PC 20. The server 16 encrypts the data key for the digital content to be downloaded using the unique identifier (and any additional information) as an encryption key (step 308). While any suitable encryption algorithm may be utilized at step 308, the data encryption is preferably performed using the well known Blowfish encryption algorithm. The Blowfish encryption algorithm is advantageously fast, especially when implemented on 32-bit microprocessors with large data caches, such as the Intel Pentium and the IBM/Motorola PowerPC. Briefly, Blowfish is a variable-length key, 64-bit block cipher which may be implemented in either hardware or software. The algorithm consists of two parts: a key-expansion part and a data-encryption part. The key expansion part converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network, wherein each round consists of a key-dependent permutation and a key- and data-dependent substitution. All operations are exclusive ORs (XOR) and additions on 32-bit words. The only additional operations are four indexed array data lookups per round to generate the encrypted data.

In accordance with the present invention, the server 16 may store digital content to be downloaded in an encrypted or unencrypted format. If the digital content to be downloaded is not stored in an encrypted format, then it is preferably encrypted upon downloading using the unique identifier as an encryption key. If the digital content to be download is stored on the server 16 in an encrypted format (pre-encrypted) prior to downloading then the server would need only to encrypt the data key to the content (i.e., the software application, music or video). Pre-encryption may be preferable to provide greater performance in environments where large amounts of data need to be encrypted per transaction. Such electronic distribution systems may be heavily burdened if they were required to encrypt the entire content that is to be electronically distributed. However, it may be preferable to double encrypt the downloaded content at step 308 by encrypting the pre-encrypted content and the data key to the pre-encrypted content using the unique identifier (and any additional information) as an encryption key. Such a technique would greatly increase the security of the data to be transmitted, as the data may be double encrypted prior

- 21 -

example, a kiosk may be provided at retail outlets where purchasers may insert a piece of media 28 into the kiosk and download data to be used on a home or office personal computer.

Referring now to Figure 9, there is illustrated the processes performed during a reading/execution/playback of the protected data once it has been written to the media 28.

5 As will be appreciated by those of skill in the art, the process of Figure 9 may be executed in multiple threads to increase the performance of the playback/execution/viewing process. As will be described below, the protected data is decrypted using the unique identifier of the media 28 as a decryption key in order to present the PC 20 or stand alone device 22 with usable electronic data.

10 The playback/execution/viewing process begins at step 320 when the user places the media 28 within the PC 20 or stand alone device 22 and accesses the protected electronic data on the media 28. The user may access the protected data using a combination of software and hardware installed on the PC 20 or stand alone device 22.

At step 322 the PC 20 (or stand alone device 22) reads the unique identifier  
15 from the media 28 and stores the unique identifier in RAM 64 (RAM 39). As noted above, the media is preferably the Iomega ZIP® disk which contains the unique serial number on a predetermined track of each ZIP® disk; however, the media is not limited to the ZIP® disk and may comprise any media having an associated unique identifier. Also as noted above, the PC 20 software may utilize the Iomega Ready API to read the serial number at step 322 from the  
20 disk.

At step 324 the PC 20 (or stand alone device 22) decrypts a predetermined string contained on the media 28 using the unique identifier. The predetermined string is compared to a known string at step 326 to determine if a proper string is decrypted (i.e., the decrypted predetermined string equals the known string). If the predetermined string has been  
25 decrypted into the known string, the process continues at step 328 where the encrypted protected electronic data is read from the media 28. Otherwise, if the result of the decryption of the predetermined string was not the known string, then all threads end, stopping the playback/execute/viewing process at step 344.

At step 328 the PC 20 (or stand alone device 22) reads the encrypted data from  
30 the media 28 and temporarily stores the protected electronic data in RAM 64 (RAM 39). The reading process may be performed within a first thread running on the PC 20, and is

- 23 -

Thus, by implementing the processes of Figure 9 in multiple threads, the processes of reading, decrypting and executing/playing/viewing the protected data may occur simultaneously in the PC 20 to increase performance.

It is noted that the PC/workstation 20 and stand alone device 22 have been  
5 described above as performing steps 320-344 in a similar fashion. However, because the PC/workstation 20 comprises a general purpose computer, there may be additional features of the present invention provided within the PC/workstation 20, which will be described below.

For example, When executing/playing/viewing the protected data on the  
10 PC/workstation 20, the software or hardware decryption process at steps 334 through 338 may be performed such that the protected electronic data is decrypted and an executable program is automatically launched to utilize the decrypted protected electronic data. Alternatively, the software or hardware decryption process may decrypt and validate the protected electronic data at steps 334 and 336 and store the decrypted data temporarily on the media 28, other  
15 media (e.g., hard disk 76) or in memory (e.g., RAM 64) for execution or use by other software or hardware applications at step 338. This alternative allows the user to play/execute/view the protected electronic data at a time after decrypting. In addition, if enhanced security is preferred, the protected electronic data could be stored in an encrypted form in RAM 64 at step 328 and temporarily decrypted at step 334 on an as-needed basis.

20 As noted above, the decryption process at step 334 (Figure 9) may be implemented in software or hardware. An exemplary first hardware implementation will be described with reference to Figures 2-4. As is well known in the art, an ASIC is a custom or semi-custom integrated circuit that may be designed to perform a variety of functions. Accordingly, the ASICs 108 and/or 36 may be designed to perform the decryption of step 334  
25 in addition to the other functions performed by ASICs 108 and 36 noted above. It is preferable to implement the decryption process in the ASIC 108 and/or 36 to minimize the likelihood of unscrupulous pirates "hacking" the decryption software for the purpose of making illegal copies of the protected electronic data.

In the first hardware embodiment, the entirety of steps 320-344 of Figure 9 are  
30 performed within a single device (e.g., PC/workstation 20 or stand alone device 22). When the first hardware embodiment is implemented in PC 20, the encrypted data read from the

- 25 -

having an associated unique identifier. The PC 20 software may utilize the Iomega Ready API to read the serial number from the disk, as noted above. At step 456 the decryption/decoding device 30 generates an authentication code, which is passed back to the PC 20 (media drive 52) at step 458. At step 460 the media drive 52 verifies that the 5 authentication code passed from the decryption/decoding device 30 is the same as the unique serial number on the media 28 actually in the drive 52. If the authentication code does not correspond to the unique identifier, then the playback/execution/viewing process stops at 468. If the authentication code matches the unique identifier, then at step 462, the media drive 52 generates a verification code. The verification code is sent to the decryption/decoding device 10 30 at step 464 and the process returns to step 404 in Figure 10A. The two-step verification process of Figure 10B ensures that the unique identifier of the media 28 physically in the media drive 52 has the same unique identifier sent to the decryption/decoding device 30 at step 454 and further enhances the present invention's resistance to hacking. The unique identifier is stored in RAM 39 for use as the decryption key in the decryption process (steps 15 406 and 412).

Referring again to Figure 10A, at step 404 the decryption/decoding device 30 decrypts a predetermined string contained on the media 28 using the unique identifier. The predetermined string is sent to the decryption/decoding device 30 via the USB/parallel/serial port 58. The predetermined string is compared to a known string by the decryption/decoding 20 device 30 at step 406 to determine if a proper string is decrypted (i.e., the decrypted string equals the known string). If the decrypted predetermined string equals the known string, the process continues at step 408 where the encrypted data is read from the media 28. Otherwise, if the decrypted predetermined string does not equal the known string, then the process ends at step 424.

At step 408, the encrypted data is read from the media 28 and sent via 25 USB/parallel/serial port 58 to the decryption/decompressing device 30 at step 410. At step 412, the ASIC/controller 36 decrypts the protected electronic data received by controller 34. The decryption process is performed as noted above with reference to step 334 (Figure 9). As the protected electronic data is decrypted, the ASIC/controller 36 (or application software 30 running on the PC 20) determines at step 414 the type of information that comprises the

protected electronic data may be read/played on any device capable of reading the media. Thus, the protected electronic data becomes portable and is tied only to a single removable media, allowing the protected electronic data to be shared while preventing the protected electronic data from being copied and read/played from another media. Further, present

5. invention may be used in a single encryption method or multiple encryption method where the key to the protected electronic data itself is encrypted using the serial number of the disk as the key.

It is noted that the foregoing examples have been provided merely for the purpose of explanation and are in no way to be construed as limiting of the present invention.

10 While the invention has been described with reference to preferred embodiments, it is understood that the words which have been used herein are words of description and illustration, rather than words of limitations. Further, although the invention has been described herein with reference to particular means, materials and embodiments, the invention is not intended to be limited to the particulars disclosed herein; rather, the invention extends

15 to all functionally equivalent structures, methods and uses, such as are within the scope of the appended claims. Those skilled in the art, having the benefit of the teachings of this specification, may effect numerous modifications thereto and changes may be made without departing from the scope and spirit of the invention in its aspects.

For example, fixed media having a unique identifier may be utilized by the

20 present invention to receive protected electronic data. Also, the removable media need not be a removable media cartridge, but may comprise a removable drive, such as those which are removably connected to personal computers or other devices via, e.g., drive bays, device bays, and PCMCIA slots.

- 29 -

5. The method as recited in claim 4, wherein said additional information comprises at least one of a purchaser's identification, address, telephone number, and payment information.

6. The method as recited in claim 1, wherein said encrypting of said electronic  
5 data to be transmitted to the client device comprises encrypting at least one of said electronic data and an encryption key to said electronic data, said encrypting using said unique identifier as an encryption key.

7. The method as recited in claim 6, further comprising:  
communicating additional information to the remote server; and  
10 encrypting additional information together with said electronic data, said additional information comprising at least one of a purchaser's name, address, telephone number, and payment information.

8. The method as recited in claim 6, wherein said encryption is performed using the Blowfish algorithm.

15 9. The method as recited in claim 1, wherein said electronic data is written to said one piece of destination media in an encrypted format using said unique identifier as a decryption key.

10. The method as recited in claim 1, wherein said establishing a connection between the client device and the server via the network infrastructure comprises:  
20 submitting, from the client device, a form to the server;  
executing, at the server, a program to process said form; and  
sending, to the client, a metatag and transaction file.

25 11. The method as recited in claim 10, wherein said metatag and said transaction file launch a client program at the client device after being sent to the client device.

- 31 -

19. The method as recited in claim 18, further comprising:  
communicating, from said second device to said first device, an authentication code to said first device;

reading, at said first device, said unique identifier from said media;  
5 comparing said authentication code to said unique identifier, and if said authentication code equals said unique identifier, generating a verification code which is communicated to said second device.

20. The method as recited in claim 15, further comprising:  
reading a predetermined string from said media;  
10 decrypting said predetermined string;  
comparing said predetermined string with a known string; and  
halting said method if said predetermined string does not equal said known string.

15 21. A system for distribution of electronic data over a network infrastructure,  
comprising:

at least one client device for operation by a user desiring to receive said electronic data; and  
20 at least one server, said at least one server containing said electronic data and offering said electronic data for downloading to said at least one client device via said network infrastructure,

wherein said at least one client device communicates a unique identifier to said at least one server, said unique identifier being associated with a particular piece of media to which said electronic data is to be stored,

25 wherein said at least one server encrypts said electronic data using said unique identifier as a key and downloads the encrypted electronic data to said at least one client computer, and

30 wherein said at least one client computer writes the encrypted electronic data to said particular piece of media such that the encrypted electronic data may only be accessed from said particular piece of media.

- 33 -

28. The apparatus as recited in claim 27, further comprising an application specific integrated circuit, wherein said application specific integrated circuit performs said decryption.

29. The apparatus as recited in claim 28, further comprising an analog to digital converter, wherein said application specific integrated circuit decompresses said electronic data and said analog to digital converter converts said decompressed electronic data into audio signals.

30. The apparatus as recited in claim 27, said media drive further comprising an application specific integrated circuit, wherein said application specific integrated circuit performs said decryption, and said decrypted electronic data is passed to said apparatus.

31. The apparatus as recited in claim 27, wherein said media drive reads a predetermined string from said media, and said processor decrypts said predetermined string and compares said predetermined string with a known string, and  
wherein said apparatus is halted if said predetermined string does not equal  
15 said known string.

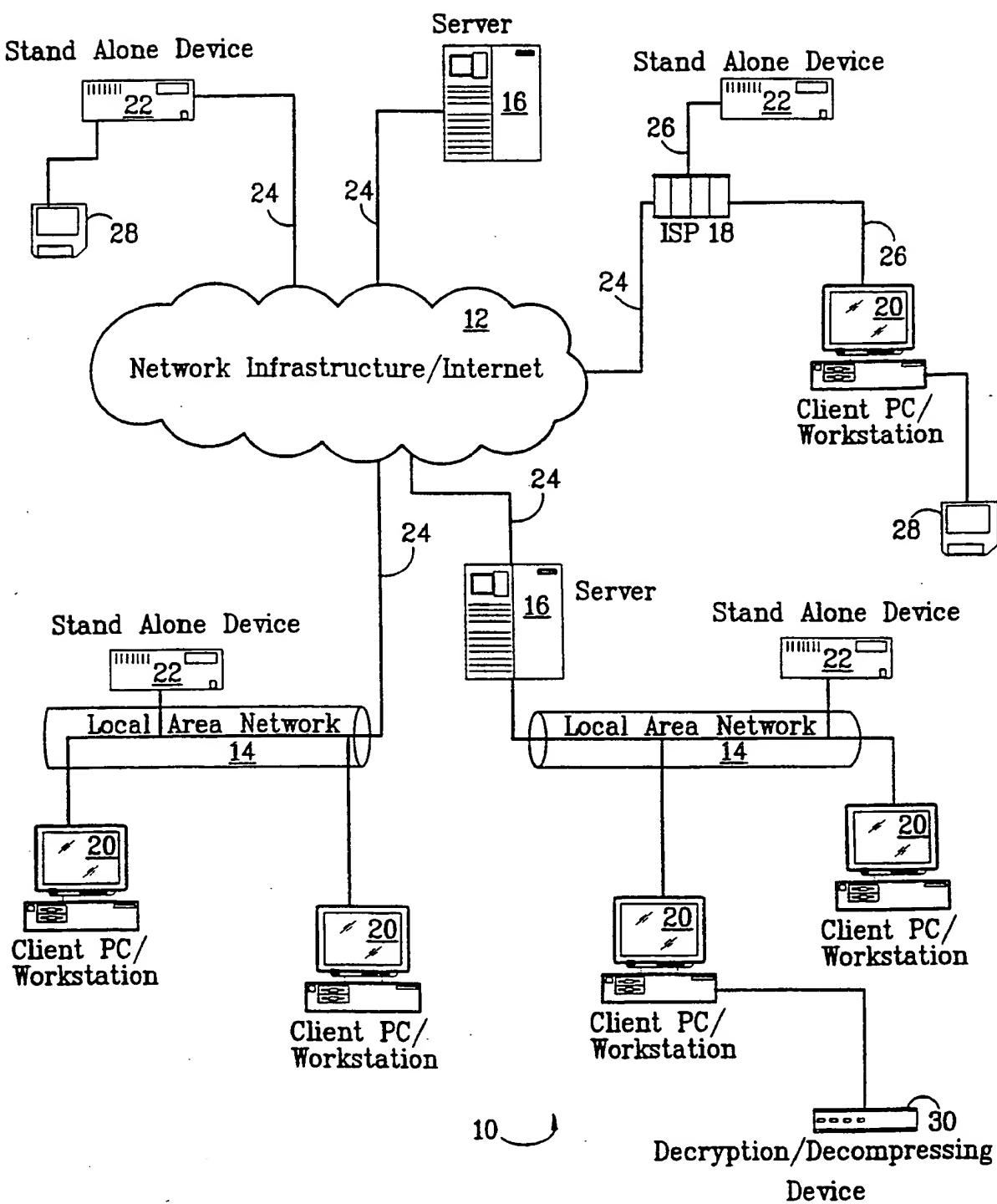
32. The apparatus as recited in claim 27, wherein said unique identifier is located on a predetermined track of said one piece of media.

33. An apparatus for reading encrypted electronic data associated to one piece of media by a unique identifier contained on said one piece of media, said apparatus being connected to a general purpose computer having a media drive which reads said unique identifier and said electronic data from said one piece of media, said apparatus comprising:  
an application specific integrated circuit which controls and executes instructions to accept said electronic data and said unique identifier from said general purpose computer;

25 wherein said electronic data is decrypted for use by said apparatus using said unique identifier as a data key, and

1/11

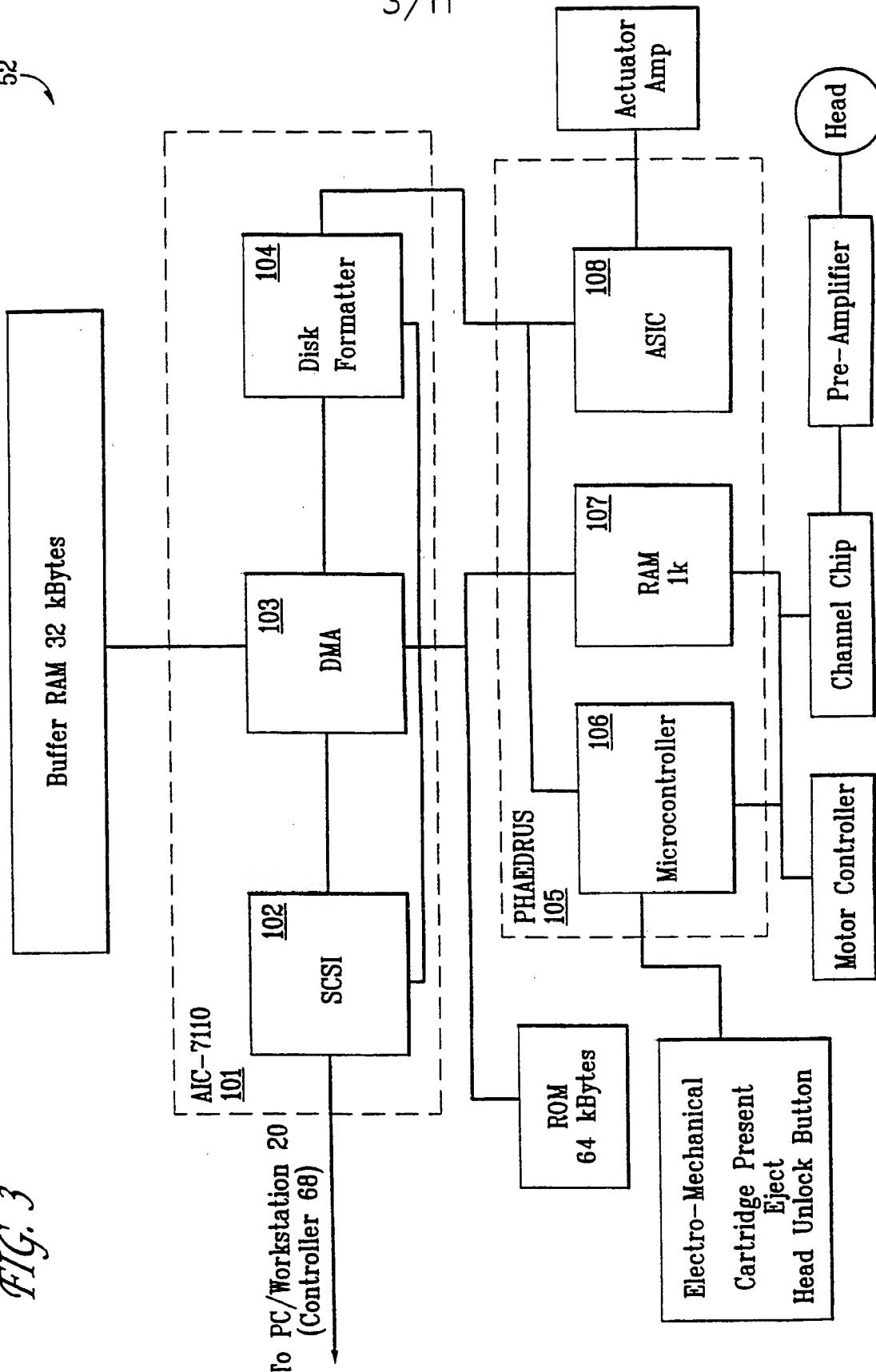
FIG. 1



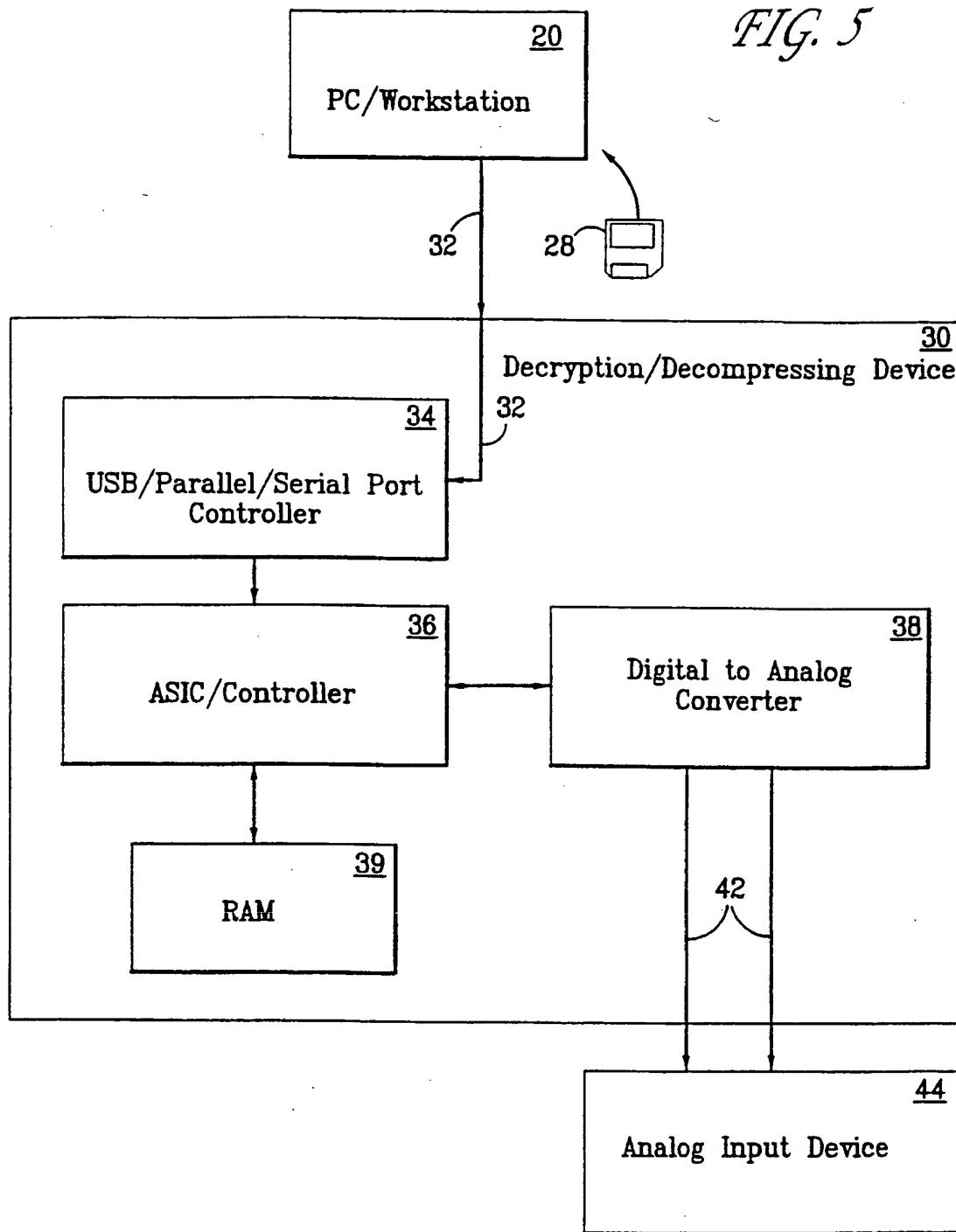
3/11

52

FIG. 3



5/11



7/11

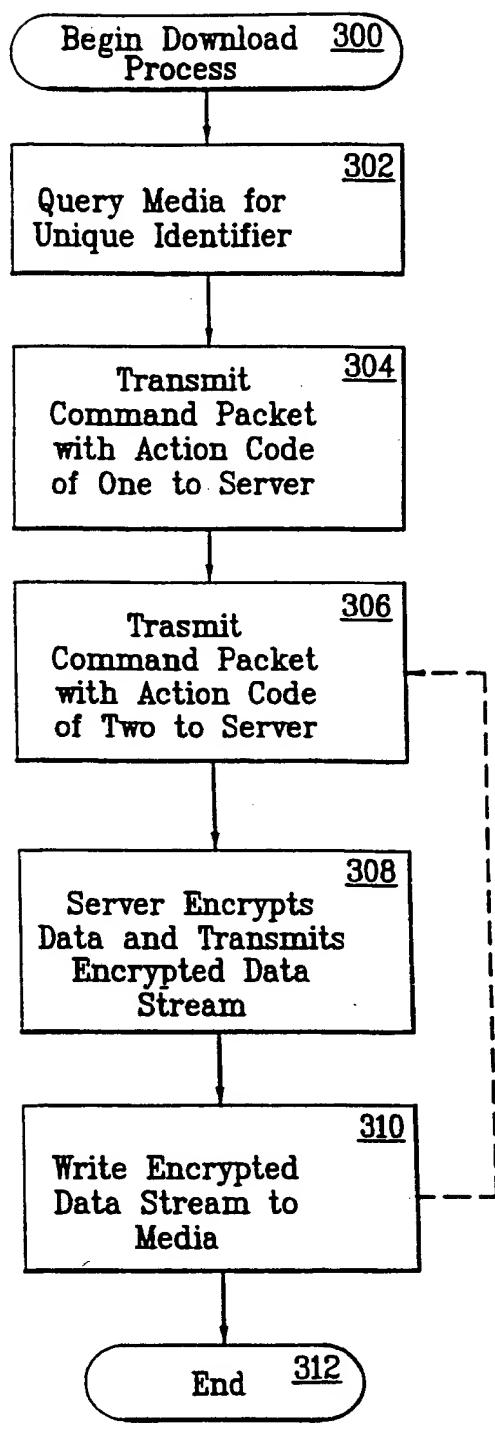
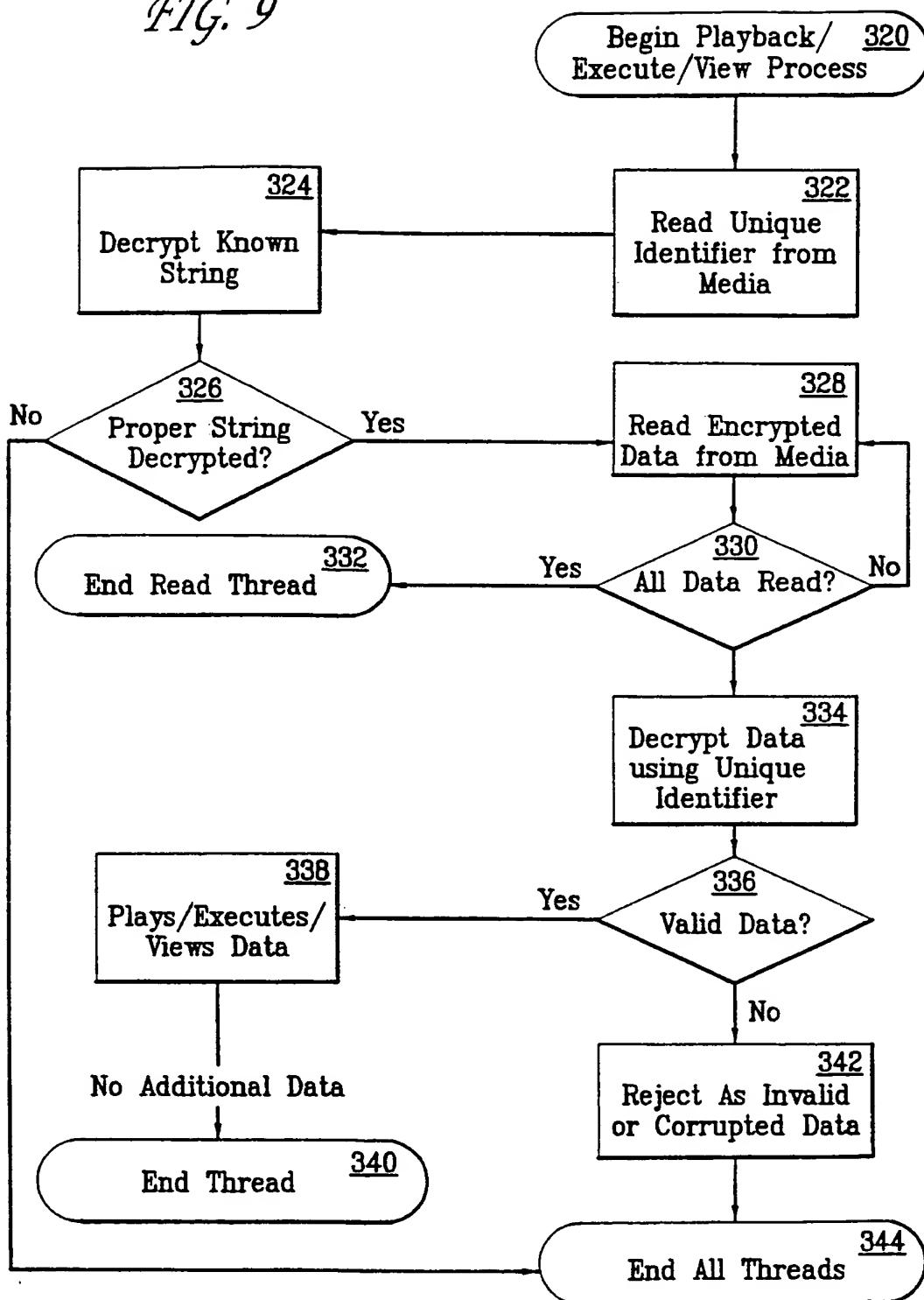


FIG. 7

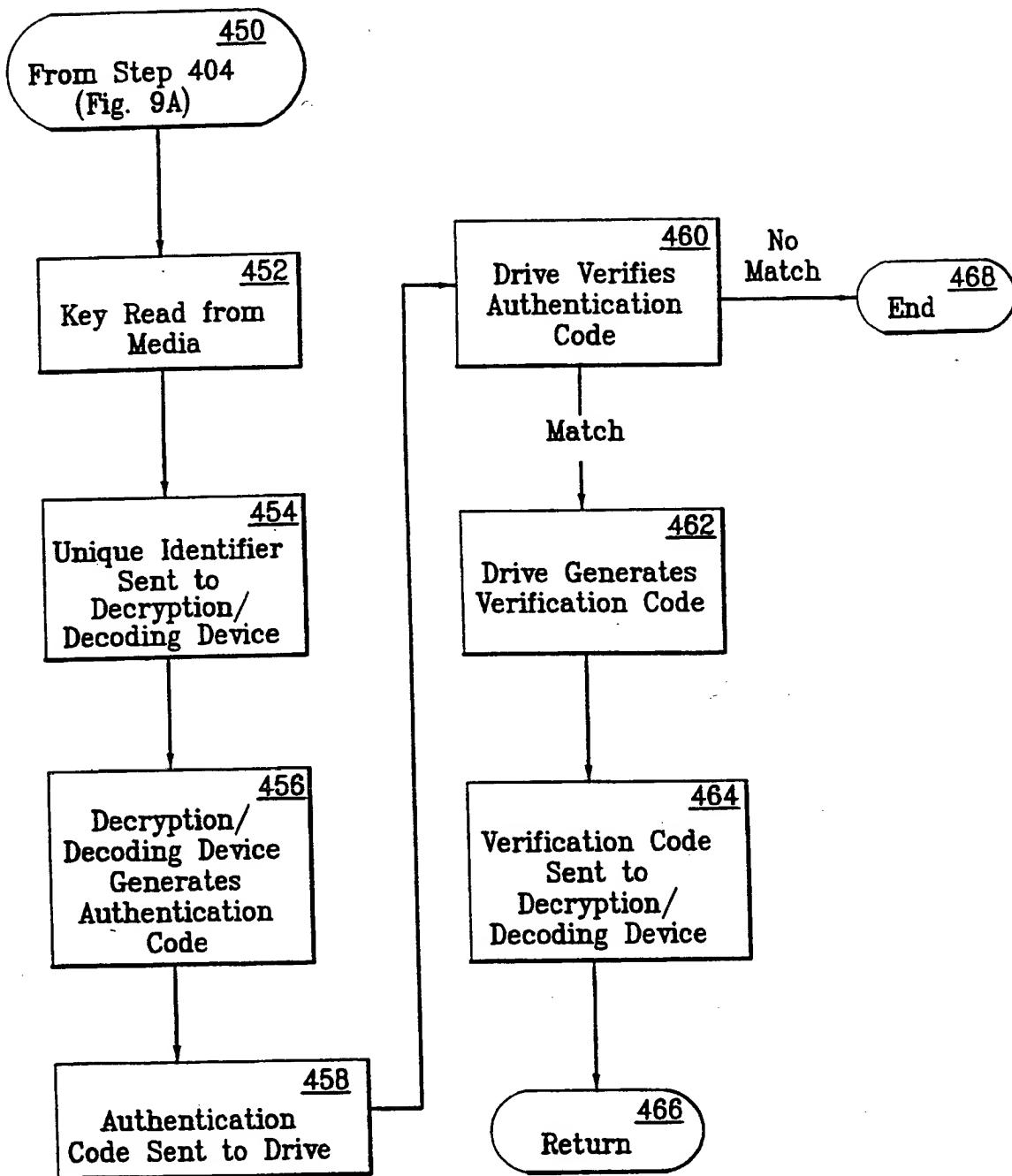
9/11

FIG. 9



11/11

FIG. 10B



## INTERNATIONAL SEARCH REPORT

International Application No PCT/US 99/08196
---

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 29416 A (INTEGRATED TECH AMERICA ;BRADLEY JAMES V (US); MOONEY DAVID M (US)) 14 August 1997 (1997-08-14) page 1, line 23 - page 3, line 5; figure 1 ---	1-3
A	WO 98 02793 A (ALLIED SIGNAL INC) 22 January 1998 (1998-01-22) page 3, line 9 - line 25; figures 3,4 ---	1
A,P	WO 98 43398 A (SENG ULRICH) 1 October 1998 (1998-10-01) page 3-5 ---	1
A,P	PATENT ABSTRACTS OF JAPAN vol. 099, no. 003, 31 March 1999 (1999-03-31) & JP 10 333769 A (MITSUBISHI ELECTRIC CORP), 18 December 1998 (1998-12-18) abstract ---	1
A	US 5 553 143 A (TAYLOR NEIL W ET AL) 3 September 1996 (1996-09-03) the whole document -----	1

THIS PAGE BLANK (USP&W)